BIZCOMMUNITY

Unlocking the web's untold censorship stories

By Madeline Earp

31 Oct 2019

The internet is not one network, but thousands of interconnected networks. How can anyone know how they are controlled without inspecting them all? In 2012, the Open Observatory of Network Interference (OONI) set out to do just that. A program run by the Seattle-headquartered Tor Project, OONI created OONI Probe, software that anyone can use to investigate their own network for signs of censorship. In 2016, the program launched OONI Explorer, a website that compiles the resultant measurements for public access.

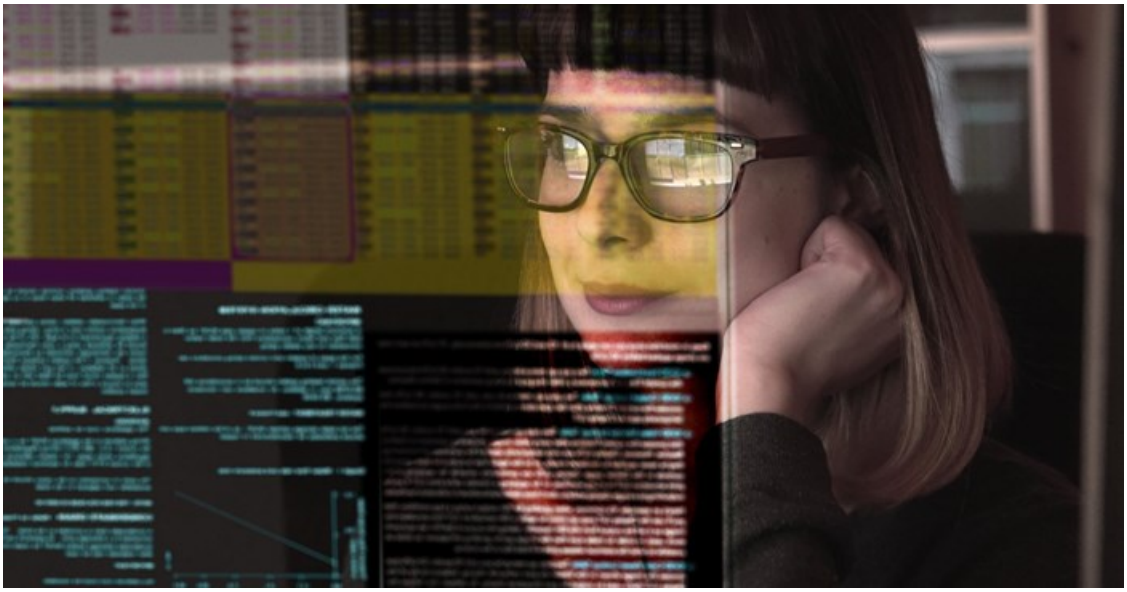

Image source: Gallo/Getty.

On September 12, OONI released a revamped OONI Explorer to help journalists and researchers explore the data. Maria Xynou, who manages research and partnerships for OONI, Arturo Filastò, the project lead, and Sarath Madayil Sreedharan, the lead developer of OONI Explorer, convened for an online chat with CPJ about the changes they've made and how they're lifting the curtain on internet censorship. [The interview has been edited for length and clarity.]

Q: Tell us about OONI Explorer and why you are relaunching it.

A: Xynou: OONI Explorer is a public internet censorship archive that is expanding with every network measurement collected and published. This allows people to track censorship changes in hundreds of countries back to 2012. We wanted to make it more usable and make the process of exploring the data more dynamic.

Q: How could journalists make use of OONI Explorer?

A: Xynou: It's very useful for confirming reported blocks. We often hear that websites or apps are inaccessible, but there so many reasons why that might be, often nothing to do with the government ordering an internet service provider (ISP) to block access. OONI Explorer can help enhance the credibility of reporting by providing evidence of censorship events and how they are occurring.

And it's a goldmine. There are so many unreported censorship stories just sitting there in the database that journalists can discover and bring to the public.

Q: How should journalists describe where data comes from?

A: Filastò: OONI Probe software is free and open source, and anyone can review how each test is designed and what it measures.

Journalists can link directly to network measurement data, or to the filtered search results. Enter a domain in the search page to see if there are any measurements in a target country. If there are, that data is collected by volunteers running tests on the ground with OONI Probe. By default, we don't collect their IP addresses. The type of collected information includes the test time, whether it was on mobile or Wi-Fi, country code, and the network's autonomous system number (ASN).

Q: What does the ASN reveal?

A: Filastò: In simple terms, any ISP like Verizon or T-Mobile will have one or more associated ASN. It may not be clear which company or brand it corresponds to, but you can find out.

Xynou: The easiest way is to Google an ASN number to check which ISP corresponds to it.

Q: What can OONI Explorer tell us about the reasons content is blocked?

A: Xynou: To determine intent, it's important to get into the nitty gritty of how. OONI Explorer measurements show which censorship techniques are adopted by ISPs (i.e. how websites and apps are blocked).

Filastò: People might know my name but still need a phone book to call me. Websites also have a digital IP address like 104.20.62.188 which corresponds to a domain name like cpj.org. ISPs may change, or spoof the address in order to send you somewhere else on government orders. So instead of using a trusted phone book, you're using the government's. Instead of speaking to me, if I'm on the block list, you're speaking to the government.

We test for this by taking steps a web browser would take to visit a website, to see if we detect interference, and repeat each test from a control location that we know is not censored. None of them is 100% precise, so false positives can arise.

The first stage resolves a domain name into an IP address. The second stage establishes what's called a TCP session, which is a connection directed towards that IP address. Then we see if we can retrieve the webpage. We apply a series of rules to understand if what we're seeing looks like a real website or a block page.

Q: What's the significance of the block page?

A: Filastò: It's what you see when you try to access blocked content in some countries, usually a notification that it's illegal. We collect fingerprints of known block pages and detect them when measurements are uploaded.

Xynou: We don't know all the block pages, and not every country uses one. But OONI Explorer describes incidents where ISPs served a block page as "confirmed" censorship. All other failures to connect are called "anomalies." Something went wrong that may involve censorship, but the website may be inaccessible for other reasons.

Q: What can anomalies tell us?

A: Xynou: One anomaly may be a false positive. But in the new search tool, you can see if other recent test results are consistent, which makes it more likely it was blocked. Let's say you're testing a news website that is blocked in Egypt. They don't serve block pages, but the failure to connect is still relevant in a larger data set or timeline, suggesting that the site in question is possibly blocked. We share the raw network measurement data to enable the public to explore further.

Q: Can journalists also test for censorship themselves?

A: Xynou: Absolutely. You can install OONI Probe on a mobile phone, on Android or iOS. There's an older version of

OONI Probe for Linux and macOS. We're launching a desktop app for Windows and macOS very soon, so stay tuned!

Most tests automatically use two standard lists of websites, one global content like Facebook and the BBC, the second relevant to the country from which you run OONI Probe. Or you can manually enter sites to test.

You can also coordinate testing in another country by adding a URL and generating an OONI Run link to send to a local OONI Probe user. But it's important to communicate about potential risks.

Q: What risks should journalists be aware of when running tests?

A: Sreedharan: One thing to remember is that journalists in conflict zones or other hotspots might be running virtual private networks (VPNs) to disguise their location. Running OONI Probe would test the VPN, not the local network, but turning the VPN off comes with other risks.

Xynou: OONI Probe is an investigative tool, not a privacy tool. Anyone monitoring your connectivity, like an ISP or government agency, will know that you're running it. To our knowledge, no laws specifically prohibit it, but authorities could try and bring it under broader national security laws.

It also depends what you're testing. A billion people connect to WhatsApp servers daily, so that's probably less risky than connecting to an illegal website. You can opt out of publishing results if you fear someone may be able to link them back to you.

We've had legal consultation, we have documentation on our website, and you have to respond correctly to a quiz about potential risks when you install the app. This is our attempt to educate people and acquire consent. We're not aware of cases where anyone got into trouble, and we really hope it stays that way.

Q: What can journalists do if they don't get the expected result, or can't interpret it?

A: Xynou: We're happy to answer questions. Any feedback or questions you may have are very valuable because we're constantly trying to improve our tools.

Filastò: Journalists should also reach out if they have any needs related to analysis. The database powering OONI Explorer is also available, with instructions for setting it up. We have terabytes of open data, and we're always happy to collaborate.

**Contact OONI Explorer via their website or Slack channel.]*

From CPJ's Emergencies Response Team: Journalists interested in using OONI probe in the country where they reside should consider whether it is safe if they have previously been targeted by a government or have concerns for their safety. For more information on digital safety, consult CPJ's Digital Safety Kit.

ABOUT THE AUTHOR

Madeline Earp is Consultant Technology Editor, the Committee to Protect Journalists.